

Making the Business Case for Software Assurance

Nancy R. Mead, Software Engineering Institute [vita¹]

Copyright © 2006, 2008 Carnegie Mellon University

2007-02-06; Updated 2009-09-10

E, L, M²

It is essential to be able to make a cost/benefit argument in order to justify investment in software assurance during the software development process. Although we are making some strides in identifying costs, quantifying the benefits can be much more elusive. In this article we give an overview of the Business Case content area.

The Status Quo

As software developers and software managers, we all know that when we want to introduce new approaches in our development processes, we have to make a cost/benefit argument to our executive management to convince them that there is a business or strategic return on investment. Executives are not interested in investing in new technical approaches simply because they are innovative or exciting. For profit-making organizations, we need to make a case that demonstrates we will improve market share, profit, or other business elements. For other types of organizations we need to show that we will improve our software in a way that is important—in a way that adds to the organization's prestige, that ensures the safety of troops in the battlefield, and so on.

In the area of software assurance, particularly security, we have started to see some evidence of successful ROI or economic arguments for security administrative operations, such as maintaining current levels of patches, establishing organization entities such as CSIRTs³ to support security investment, and so on [Blum 2006⁴, Gordon 2006⁵, Huang 2006⁶, Nagaratnam 2005⁷]. Initially there were only a few studies [Soo Hoo 2001⁸, Berinato 2002⁹, Jaquith 2002¹⁰] that presented evidence to support the idea that investment during software development in software security will result in commensurate benefits across the entire life cycle. This picture has improved, however. As we expected early on, Microsoft has published data reflecting the results of using their Security Development Lifecycle [Howard 2006¹¹]. Microsoft is using the level of vulnerabilities and therefore the level of patches needed as a measure of improved cost/benefit [Microsoft 2008¹²]. The reduced level of patches/vulnerabilities in recent Microsoft product releases is remarkable. In addition, Microsoft has recently published a white paper describing a method of calculating ROI for investments in security during the development life cycle [Microsoft 2009¹³].

We would also refer readers to the Business Context discussion in Chapter 2 and the Business Climate discussion in Chapter 10 of McGraw's recent book [McGraw 2006¹⁴] for ideas. There has been some work on a security-oriented version of COCOMO called COSECMO¹⁵; however, the focus has been more on cost

-
1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/230-BSI.html (Mead, Nancy)
 3. <http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/incident/662-BSI.html> (Defining Computer Security Incident Response Teams)
 4. #dsy685-BSI_blum2006
 5. #dsy685-BSI_gordon2006
 6. #dsy685-BSI_huang2006
 7. #dsy685-BSI_nagaratnam2005
 8. #dsy685-BSI_soo2001
 9. #dsy685-BSI_berinato2002
 10. #dsy685-BSI_jaquith2002
 11. #dsy685-BSI_howard2006
 12. #dsy685-BSI_microsoft2008
 13. #dsy685-BSI_microsoft2009
 14. #dsy685-BSI_mcgraw2006
 15. http://sunset.usc.edu/events/2006/CIIForum/pages/presentations/outbrief%20-%20Costing-Secure-Systems-Workshop-Report.2006%20_Nov_07.ppt

estimation than on return on investment. Reifer is also working in this area on a model called CONIPMO, which is aimed at systems engineers [Reifer 2006¹⁶]. Data presented by Fortify¹⁷ indicates that the cost of correction of security flaws at the requirements level is up to 100 times less than the cost of correction of security flaws in fielded software. COCOMO data suggests that the cost of fixing errors of all types at requirements time is about 20 times less than the cost of fixing errors in fielded software. Regardless of which statistic is used, there would seem to be a substantial cost savings for fixing security flaws at during requirements development rather than fixing security flaws after software is fielded. For vendors, the cost is magnified by the expense of developing and releasing patches. However, it seems clear that cost savings exist even in the case of custom software when security flaws are corrected early in the development process.

At this time there is little agreement on the right kinds of models to be used for this purpose, and although there is now case study data that supports the ROI argument for investment in software security early in software development, there is still very little published data.

On the other hand, Bruce Schneier¹⁸ believes that it is not feasible to accurately calculate the benefit that is derived from improved security. He points out that there is very little actual data on the cost of a break-in and that predicting the cost of a rare but damaging event is fraught with peril. In this article he summarizes his position on calculating security ROI as follows: "It's a good idea in theory, but it's mostly bunk in practice."

Our belief is that even though they may not constitute a traditional ROI argument, the methods being used to calculate cost/benefit, whether they be reduced levels of patching in the field or reduced cost of fixing security flaws when they are found early in the lifecycle, are convincing.

What We Can Offer

Given this state of affairs, we are unable to recommend a single model for calculating cost/benefit for early investment in software security during software development. Instead, we find that we are able to describe a variety of models that may be useful for calculating software assurance valuation. In the article by Shoemaker et al., Models for Assessing the Cost and Value of Software Assurance¹⁹, we present models that could be considered by organizations who are thinking of investing in software assurance. More recently, an article by Shoemaker et al., A Common Sense Way to Make the Business Case for Software Assurance²⁰, provides a practical approach for arriving at a cost/benefit argument. The article by Arora et al., Estimating Benefits from Investing in Secure Software Development²¹, specifically addresses a way of estimating cost and benefits associated with improved security. Don O'Neill provides the article Calculating Security Return on Investment²², which describes several approaches to calculating security return on investment and gives detailed examples. O'Neill's article Business Considerations and Foundations for Assuring Software Security: Business Case Models for Rational Action²³ discusses business considerations and business case models for assuring software security. The O'Neill article Maturity Framework for Assuring Resiliency Under Stress²⁴ specifies a framework for assuring the resiliency of the critical infrastructure through a management, process, and engineering framework.

16. #dsy685-BSI_reifer2006

17. <https://buildsecurityin.us-cert.gov/swa/downloads/Meftah.pdf>

18. http://www.schneier.com/blog/archives/2008/09/security_roi_1.html

19. <http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/684-BSI.html> (Models for Assessing the Cost and Value of Software Assurance)

20. <http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/952-BSI.html> (A Common Sense Way to Make the Business Case for Software Assurance)

21. <http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/267-BSI.html> (Estimating Benefits from Investing in Secure Software Development)

22. <http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/677-BSI.html> (Calculating Security Return on Investment)

23. <http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/676-BSI.html> (Business Considerations and Foundations for Assuring Software Security: Business Case Models for Rational Action)

24. <http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/1016-BSI.html> (Maturity Framework for Assuring Resiliency Under Stress)

Recent Developments

In 2008 we conducted a [Workshop on Business Case](#)²⁵ and all indications are that at present there is no single common model that is widely accepted. Many issues and approaches were presented at the workshop, which had more than 70 attendees internationally from industry, government, and academe.

As noted above, Microsoft is using the level of vulnerabilities and patches needed as a measure of improved cost/benefit, and data presented by Fortify is using the comparative cost of correction of security flaws at various points in the software life cycle.

In 2009 we published a guide for “[Making the Business Case for Software Assurance](#)²⁶.” Although there is no single model that can be recommended for making the cost/benefit argument, there are promising models and methods that can be used individually and collectively for this purpose, as well as some convincing case study data that supports the value of building software assurance into newly developed software. These are described in the guide.

References

- | | |
|------------------|---|
| [Berinato 2002] | Berinato, S. “Finally, a Real Return on Security Spending.” <i>CIO Magazine (Australia)</i> , August 4, 2002. |
| [Blum 2006] | Blum, D. <i>Making Business Sense of Information Security, Security and Risk Management Strategies</i> . Burton Group, Version 1.0, February 10, 2006. |
| [Gordon 2006] | Gordon, L. A. & Loeb, M. P. “Budgeting Process for Information Security Expenditures.” <i>Communications of the ACM</i> 49, 1 (January 2006): 121-125. |
| [Howard 2006] | Howard, Michael & Lipner, Steve. <i>The Security Development Lifecycle</i> . Redmond, WA: Microsoft Press, 2006. |
| [Huang 2006] | Huang, C.D.; Hu, Q.; & Behara, R. S. “Economics of Information Security Investment in the Case of Simultaneous Attacks.” <i>The Fifth Workshop on the Economics of Information Security (WEIS 2006)</i> . University of Cambridge, England, June 26-28, 2006. |
| [Jaquith 2002] | Jaquith, Andrew. <i>The Security of Applications: Not All Are Created Equal</i> ²⁷ (@atstake Security Research Report) (2002). |
| [McGraw 2006] | McGraw, Gary. <i>Software Security: Building Security In</i> . Upper Saddle River, NJ : Addison-Wesley, 2006. |
| [Microsoft 2008] | MSDN. The Microsoft Security Development Lifecycle (SDL): Measurable Improvements for Flagship Microsoft Products ²⁸ , 2008. |
| [Microsoft 2009] | Microsoft Corp. <i>Microsoft SDL: Return on Investment</i> ²⁹ . September 15, 2009. |

25. https://buildsecurityin.us-cert.gov/swa/downloads/BCW_Proceedings.pdf

26. <http://www.sei.cmu.edu/library/abstracts/reports/09sr001.cfm>

[Nagaratnam 2005]

Nagaratnam, N.; Nadalin, A.; Hondo, M.; McIntosh, M.; & Austel, P. "Business-driven application security: From modeling to managing secure applications." *IBM Systems Journal* 44, 4 (2005): 847-867.

[Reifer 2006]

Reifer, Donald. "[CONIPMO Workshop](#)³⁰." Practical Software Measurement Conference, Vail, CO, July 24-28, 2006.

[SooHoo 2001]

Soo Hoo, K.; Sudbury, A. W.; & Jaquith, A. R. "Tangible ROI through Secure Software Engineering." *Secure Business Quarterly* 1, 2 (Fourth Quarter 2001).

Carnegie Mellon Copyright

Copyright © Carnegie Mellon University 2005-2010.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

1. <mailto:permission@sei.cmu.edu>